K. Clark – x4859

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MARYLAND

IN THE MATTER OF THE SEARCH OF VARIOUS ELECTRONIC DEVICES (LISTED IN ATTACHMENT A) CURRENTLY AT THE DEA BALTIMORE DISTRICT OFFICE LOCATED IN BALTIMORE, MARYLAND	**Case No.** 19-4039 BPG

AFFIDAVIT IN SUPPORT OF A SEARCH AND SEIZURE WARRANT

I, DANIEL PAMER, being duly sworn, depose and state as follows:

INTRODUCTION

1. Your Affiant makes this Affidavit in support of an application under Federal Rule of Criminal Procedure 41 for a search warrant authorizing the forensic examination of two cellular telephones, five computers, and two storage cards, as described in Attachment "A" (collectively referred to as the "SUBJECT DEVICES") which are in the United States Drug Enforcement Administration's possession at the Baltimore District Office in Baltimore, Maryland, and the extraction of electronically stored information identified in Attachment "B" from those devices pursuant to the search protocol set forth in Attachment "C."

2. Investigators found and seized the SUBJECT DEVICES while executing search warrants issued by United States Magistrate Judge Martin C. Carlson of the Middle District of Pennsylvania, and arresting the target, on November 19, 2019. Therefore, while the DEA might already have all necessary authority to examine the SUBJECT DEVICES, I seek this additional warrant out of an abundance of caution to be certain that an examination of the SUBJECT DEVICES will comply with the Fourth Amendment and other applicable laws.

3. Your Affiant submits that probable cause exists to believe that the SUBJECT

DEVICES contain evidence of violations of 21 U.S.C. § 841, 846 (Distribution and Possession with Intent to Distribute Controlled Substances and conspiracy to commit the same), 21 U.S.C. § 843(b) (Use of a Communication Facility), and 18 U.S.C. § 1956 (Money Laundering) or the SUBJECT DEVICES were designed for use, intended for use, or used in committing the aforementioned crimes.

IDENTIFICATION OF THE DEVICES

4. As detailed further on Attachment A, the SUBJECT DEVICES—all of which are in the DEA's possession at the Baltimore District Office in Baltimore, Maryland—are as follows:

ITEM	DESCRIPTION	SEIZURE LOCATION
Cellphone No. 1	**Samsung Galaxy S8+ IMEI#357725084952929 (photo at Attachment "D")**	**Seized from the vehicle of Jacob LEISTER**
Cellphone No. 2	**Samsung Galaxy III Trac Phone FCC ID# A3LSCHI535 (photo at Attachment "E")**	**Seized from 4692 Blue Hill Rd. Glenville, PA**
Computer No. 1	**Dell Laptop Serial # BC05662 N-7 (photo at Attachment "F")**	**Seized from 4692 Blue Hill Rd. Glenville, PA**
Computer No. 2	**HP Laptop No Serial Number N-12 (photo at Attachment "G")**	**Seized from 4692 Blue Hill Rd. Glenville, PA**
Computer No. 3	**Dell Inspiron Laptop Serial #70MDBC1 N-13 (photo at Attachment "H")**	**Seized from 4692 Blue Hill Rd. Glenville, PA**
Computer No. 4	**Dell Laptop Serial # 1Z3RZG1 N-14 (photo at Attachment "I")**	**Seized from 4692 Blue Hill Rd. Glenville, PA**
Computer No. 5	**Samsung Galaxy Tablet Serial # A3LSMT17S (photo at Attachment "J")**	**Seized from 4692 Blue Hill Rd. Glenville, PA**
Storage No. 1	**Miscellaneous Digital Storage Cards and Sim Cards (photo at Attachment "K")**	**Seized from 4692 Blue Hill Rd. Glenville, PA**

Storage No. 2	**Sans Disk SD Card (photo at Attachment "L")**	**Seized from vehicle of Jacob LEISTER**

5. In your Affiant's training and experience, your Affiant knows that the DEA has stored the SUBJECT DEVICES in a manner in which their contents are, to the extent material to this investigation, in substantially the same state as they were when the SUBJECT DEVICES first came into the DEA's possession. The applied-for warrants would authorize the forensic examination of the SUBJECT DEVICES for the purpose of identifying electronically stored data particularly described in Attachment B.

YOUR AFFIANT

6. Your Affiant has been a sworn member of the Anne Arundel County Police Department since September 2004. He has been assigned as a Task Force Officer ("TFO") with the DEA's Tactical Diversion Squad in Baltimore, Maryland, since January 2018. In this role, your Affiant investigates criminal violations related to the diversion of pharmaceutical controlled dangerous substances and prescription medications.

7. Your Affiant has participated in numerous investigations of unlawful drug distribution involving the use of undercover officers, confidential informants, and undercover transactions. In addition, he has conducted physical surveillance, telephone toll analysis, and investigative interviews; applied for and executed search warrants; and assisted in the recovery of substantial quantities of narcotics, pharmaceutical controlled substances, proceeds thereof, and related paraphernalia. Moreover, your Affiant has interviewed individuals involved in the controlled dangerous substance ("CDS") trafficking trade, including drug dealers and users as well as confidential informants, and among the topics covered during such interviews are the habits, lifestyles, and terminology in the CDS trafficking trade.

8. Through your Affiant's training, knowledge and experience, he has become familiar with the manner in which CDS traffickers transport, store, "stash," manufacture, and distribute CDS; the methods by which such traffickers collect and conceal the proceeds of their illegal activities; and the manner in which CDS traffickers use cellular telephones and other electronic devices like computers and storage media to facilitate illegal activities and hamper law enforcement investigations.

9. Your Affiant is aware that Drug Traffickers that use the "Dark Web," or "Deep Web" can disguise their criminal activity on a computer/laptop/tablet/internet device, and hide profits received through illicit activity in the form of "Crypto Currency," or electronic monetary transactions

10. The facts set forth in this Affidavit are based upon your Affiant's personal knowledge, review of documents and other evidence related to this investigation, and communications with other individuals who have personal knowledge of the events and circumstances described herein as well as information gained through training and experience. This Affidavit does not contain all of the information known to your Affiant regarding this investigation. Your Affiant has included only the facts that are sufficient to support a probable cause finding for the issuance of the requested warrant and does not purport to include each and every matter of fact observed or known to your Affiant or other law enforcement officers involved in this investigation.

Use of Electronic Devices by CDS Traffickers

11. Based upon your Affiant's training, experience, and participation in other CDS trafficking investigations, he knows that individuals involved in drug trafficking, including those involved in the diversion of pharmaceutical drugs, often do the following:

a. Maintain books, records, and other documents that relate to the manufacture, transportation, possession, and distribution of controlled substances where they have such information readily accessible to them, including their homes, offices, and electronic devices, such as cellular telephones, computers, and related storage media.

b. Store the names, addresses, and/or telephone numbers of associates in their drug trafficking activities on cellular telephones.

c. Use cellular telephones to communicate with their customers and/or co-conspirators via voice calls and text messages. Text messages, voice messages, records of incoming and outgoing communications, emails are often stored on electronic devices such as cell phones.

d. Use multiple cellular telephones and electronic devices in an effort to conceal their activities.

e. Keep logs of drug debts owed by customers or to suppliers, commonly referred to as an "owe sheet" or a "tally sheet" on their cellular telephones or other electronic devices.

12. Based on my training and experience, I use the following technical terms to convey the following meanings:

a. Wireless telephone: A wireless telephone (or mobile telephone, or cellular telephone) is a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional "land line" telephones. A wireless telephone usually contains a "call log," which records the telephone number, date, and time of calls made to

and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic "address books;" sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may also include global positioning system ("GPS") technology for determining the location of the device.

b. Digital camera: A digital camera is a camera that records pictures as digital picture files, rather than by using photographic film. Digital cameras use a variety of fixed and removable storage media to store their recorded images. Images can usually be retrieved by connecting the camera to a computer or by connecting the removable storage medium to a separate reader. Removable storage media include various types of flash memory cards or miniature hard drives. Most digital cameras also include a screen for viewing the stored images. This storage media can contain any digital data, including data unrelated to photographs or videos.

c. Portable media player: A portable media player (or "MP3 Player" or iPod) is a handheld digital storage device designed primarily to store and play audio, video, or photographic files. However, a portable media player can also store other digital data. Some portable media players can use removable storage media. Removable storage media include various types of flash memory cards

or miniature hard drives. This removable storage media can also store any digital data. Depending on the model, a portable media player may have the ability to store very large amounts of electronic data and may offer additional features such as a calendar, contact list, clock, or games.

d. GPS: A GPS navigation device uses the Global Positioning System to display its current location. It often contains records the locations where it has been. Some GPS navigation devices can give a user driving or walking directions to another location. These devices can contain records of the addresses or locations involved in such navigation. The Global Positioning System (generally abbreviated "GPS") consists of 24 NAVSTAR satellites orbiting the Earth. Each satellite contains an extremely accurate clock. Each satellite repeatedly transmits by radio a mathematical representation of the current time, combined with a special sequence of numbers. These signals are sent by radio, using specifications that are publicly available. A GPS antenna on Earth can receive those signals. When a GPS antenna receives signals from at least four satellites, a computer connected to that antenna can mathematically calculate the antenna's latitude, longitude, and sometimes altitude with a high level of precision.

e. PDA: A personal digital assistant, or PDA, is a handheld electronic device used for storing data (such as names, addresses, appointments or notes) and utilizing computer programs. Some PDAs also function as wireless communication devices and are used to access the Internet and send and receive e-mail. PDAs usually include a memory card or other removable storage media for storing

data and a keyboard and/or touch screen for entering data. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can store any digital data. Most PDAs run computer software, giving them many of the same capabilities as personal computers. For example, PDA users can work with word-processing documents, spreadsheets, and presentations. PDAs may also include global positioning system ("GPS") technology for determining the location of the device.Tablet: A tablet is a mobile computer, typically larger than a phone yet smaller than a notebook, that is primarily operated by touching the screen. Tablets function as wireless communication devices and can be used to access the Internet through cellular networks, 802.11 "wi-fi" networks, or otherwise. Tablets typically contain programs called apps, which, like programs on a personal computer, perform different functions and save data associated with those functions. Apps can, for example, permit accessing the Web, sending and receiving e-mail, and participating in Internet social networks.

f. IP Address: An Internet Protocol address (or simply "IP address") is a unique numeric address used by computers on the Internet. An IP address is a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet computer must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static—that is, long-term—IP addresses, while other computers have

dynamic—that is, frequently changed—IP addresses.

g. Internet: The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

13. Based on my training, experience, and research, I know that **Cellphone Nos. 1 - 2** have capabilities that allow them to serve as a wireless telephone, digital camera, portable media player, GPS navigation device, and PDA. In my training and experience, examining data stored on devices of this type can uncover, among other things, evidence that reveals or suggests who possessed or used the device.

14. Based on my training, experience, and research, I know that **Computers Nos. 1 - 5** have capabilities that allow them to store data, create documents, and access the internet using IP addresses. In my training and experience, examining data stored on devices of this type can uncover, among other things, evidence that reveals or suggests who possessed or used the device.

15. Based on my training, experience, and research, I know that **Storage Nos. 1 - 2** have capabilities that allow them to store data, alter electronic telephone systems, and hide evidence. In my training and experience, examining data stored on devices of this type can uncover, among other things, evidence that reveals or suggests who possessed or used the device.

ELECTRONIC STORAGE AND FORENSIC ANALYSIS

16. Based on my knowledge, training, and experience, I know that the **SUBJECT**

DEVICES can store information for long periods of time. Similarly, things that have been viewed via the Internet are typically stored for some period of time on the device. This information can sometimes be recovered with forensics tools.

17. There is probable cause to believe that things that were once stored on **Computer Nos. 1-5 and Storage Nos. 1-2** may still be stored there, for at least the following reasons:

a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

c. Wholly apart from user-generated files, computer storage media—in particular, computers' internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating

system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory "swap" or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache."

18. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how the Device was used, the purpose of its use, who used it, and when. There is probable cause to believe that this forensic electronic evidence might be on the SUBJECT DEVICES because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). On computers, virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems

can record information about the dates files were created and the sequence in which they were created.

b. Forensic evidence on a device can also indicate who has used or controlled the device. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence.

c. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact electronically stored information on a storage medium that is necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.

19. *Nature of examination.* Based on the foregoing, and consistent with Rule

41(e)(2)(B), the warrant I am applying for would permit the examination of the SUBJECT DEVICES consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the devices to human inspection in order to determine whether it is evidence described by the warrant.

20. *Manner of execution.* Because this warrant seeks only permission to examine devices already in law enforcement's possession, the execution of this warrant does not involve the physical intrusion onto a premises. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

PROBABLE CAUSE

21. During the month of December 2018, A Confidential Source provided information to an Anne Arundel County Narcotics Detective and advised them that **Jacob LEISTER** was currently selling large quantities of the controlled drug Xanax (Xanax is a brand name for Alprazolam, a Schedule IV Controlled Substance). That Detective established contact with a phone number that was provided as **Jacob LEISTER's** cellular phone number. The number provided to the detective by the source was 302-393-2935, and the undercover detective sent text messages to this number in an attempt to contact **LEISTER**. After texting the number, the undercover detective was instructed by text message to use a messaging application known as Wickr, which is an encrypted messaging application. Using the Wickr messaging application, the detective was able to confirm that he was communicating with **LEISTER.** The detective discussed with **LEISTER** through Wickr, about making a purchase of Xanax. During conversation, **LEISTER** offered a quantity of up to 500 tablets of Alprazolam. The undercover detective arranged to meet with **LEISTER** in Anne Arundel County. At a later date in December 2018,

LEISTER met with the Undercover Detective in Anne Arundel County, Maryland, at which time **LEISTER** provided the detective with three plastic baggies containing white and yellow tablets with total of (100) rectangular tablets, suspected Alprazolam. The undercover Detective provided **LEISTER** $300.00 of marked bills from the Anne Arundel County Police Vice/Narcotics fund in exchange for the suspected Alprazolam. A lab test was conducted of the suspected Alprazolam and it was found to be Flubromazolam, a designer benzodiazepine which is currently unscheduled. Flubromazolam is not federally scheduled but has been scheduled in some states.

22. During the months of January 2019 and February 2019, the undercover detective met with **LEISTER** twice more in Anne Arundel County, Maryland. During each meeting, **LEISTER** provided 250 white and yellow tablets to the undercover detective in exchange for $700.00 US Currency. A total of 500 tablets were purchased by the detective from **LEISTER** in exchange for $1,400.00 of marked currency from the Anne Arundel County Police Vice/Narcotics fund. The tablets were again tested in the Anne Arundel County Drug Laboratory, and found to be Flubromazolam.

23. In early May 2019, the undercover detective continued communication with **LEISTER** through the Wickr application. During those communications, **LEISTER** informed the detective that he could sell Oxycodone tablets, along with the normal supply of Alprazolam. The detective again met with **LEISTER** in Anne Arundel County, Maryland, where **LEISTER** provided the detective with 45 blue tablets that **LEISTER** identified as Oxycodone 30mg, and 300 white bar shaped tablets **LEISTER** identified as 2mg Xanax tablets. The detective gave **LEISTER** $2,000.00 in marked US Currency from the Anne Arundel County Police Vice/Narcotics fund in exchange for both the Oxycodone and Xanax. The tablets were tested at the Anne Arundel County Drug Laboratory, and the blue tablets were identified as Fentanyl

pressed to look like Oxycodone 30mg, and the white bar tablets were identified as Alprazolam, the active ingredient in Xanax.

24. In late May 2019, your affiant met with the undercover detective regarding their investigation, and instructed him to reach out to **LEISTER** to arrange another purchase of Oxycodone from him. **LEISTER** agreed to sell the undercover detective more blue tablets, and in late May, your affiant conducted a controlled purchase of narcotics with **LEISTER** that was arranged by the undercover detective. **LEISTER** met with the undercover detective in Anne Arundel County, Maryland, where he provided the detective with 45 blue tablets he identified as Oxycodone 30 mg and 10 THC Oil cartridges. The undercover detective gave **LEISTER** $1,600.00 of US Currency from the Drug Enforcement Administration in exchange for the blue tablets and the THC cartridges. A lab test by the DEA's Mid-Atlantic Laboratory found that the blue tablets contained fentanyl, a schedule II controlled substance.

25. In June 2019, and July 2019 your affiant conducted two more controlled purchases of blue Oxycodone 30mg from **LEISTER** using the undercover detective. **LEISTER** met with the undercover detective once in June 2019 and once in July 2019, where he exchanged 410 tablets of blue Oxycodone for $7,000.00 US Currency from the Drug Enforcement Administration. A lab test by the DEA's Mid-Atlantic Laboratory found that the blue tablets purchased in June 2019 contained fentanyl, a schedule II controlled substance.

26. After the controlled purchase in July 2019, your affiant drove the 250 tablets of blue Oxycodone purchased by the undercover detective to the Mid-Atlantic Laboratory for a presumptive analysis. The presumptive analysis showed these tablets purchased from **LEISTER** contained Fentanyl.

27. Also during the month of August 2019, **LEISTER** communicated with the

undercover detective that multiple subjects he supplies with Xanax tablets to sell in the Westminster, Maryland area, had been arrested by local police. **LEISTER** sent the undercover detective internet web links to two different news articles describing two occasions in August 2019, where two separate individuals were arrested by local police, and had in their possession large quantities of white Xanax bars. **LEISTER** told the undercover detective that he was the supplier for these two individuals, and that he was becoming increasingly paranoid about being investigated by law enforcement.

28. In September 2019, the undercover detective communicated with **LEISTER**, and asked to meet again to satisfy a debt owed to **LEISTER**, and to purchase more Oxycodone. **LEISTER** communicated with the undercover detective that he would not sell him any more Oxycodone without a down payment sent electronically to him through either the CashApp or Venmo electronic payment applications. **LEISTER** insisted that the undercover detective use electronic payments, and communicated to the undercover detective that any future payments for Oxycodone would only be done with an electronic down payment made to **LEISTER**'s CashApp, or Venmo Account. **LEISTER** agreed to meet with the undercover detective, however, he informed the undercover detective that he would only sell him Xanax tablets. A meet with **LEISTER** was conducted at an undisclosed location in Harford County where the undercover detective provided **LEISTER** with $2,000.00 of US Currency from the Drug Enforcement Administration in exchange for satisfying owed money for the Oxycodone pressed fentanyl purchased in July 2019, and 400 tablets of white 2mg Xanax bars.

29. During October and November 2019, **LEISTER** continued communication with the undercover detective through the Wickr text messaging application about coordinating further sales of Oxycodone, and Xanax bars. **LEISTER** continued to insist that the undercover detective

conduct all future transactions for Oxycodone with an electronic cash transfer up front, through either CashApp or Venmo. **LEISTER** stated that he had supplies of Xanax and MDMA on hand that he would sell for cash.

CRYPTOCURRENCY USE BY JACOB LEISTER

30. In September 2019, a Federal Grand Jury Subpoena was served on the Abra Crypto Currency exchange for all accounts associated with **LEISTER**, and the company identified an Abra account for **LEISTER**. At the time of account creation, **LEISTER** uploaded a photograph of his driver's license as required by Abra, which showed him to have the address of 4692 Blue Hill Rd. Glenville, PA (the "**PREMISES**") on his driver's license. **LEISTER** also used the address of the **PREMISES** as the listed physical address, and Abra data showed recent account use at the end of September 2019. Abra data also showed that **LEISTER** was transferring large amounts of US Currency to the Abra exchange, and converting it to Crypto Currency. Abra data also showed that **LEISTER** had converted almost $40,000.00 of US Currency into Crypto Currency since the account's creation in May 2018.

"DARK/DEEP WEB" USE BY JACOB LEISTER

31. In June of 2019, your Affiant applied for a Search and Seizure warrant through the Anne Arundel County Circuit Court, for the social media Facebook account identified as belonging to **LEISTER**. The warrant was reviewed and signed by the Honorable William Mulford III and served on Facebook LLC.

32. Facebook returned all Facebook data requested by investigators. The Facebook data showed **LEISTER** had numerous discussions through the Facebook Messenger application with an unknown subject discussing the sale of Xanax and Anabolic Steroids over the Internet. In

the messages **LEISTER** discussed prices with the unknown subject, and was provided with a detailed price list for controlled substances for purchase through the unknown subject. **LEISTER** was also seen in Facebook messages receiving tracking information from multiple subjects regarding packages sent through the US Postal Service. **LEISTER** provided the address of the **PREMISES** each time he requested a delivery, and had photographs of USPS labels with the **PREMISES**. **LEISTER** routinely identified through Facebook that the **PREMISES** was his home address.

33. For example, **LEISTER** had the following Facebook conversations with an unknown subject using the name Bob Juiceton:

a. Month of December 2018 – **LEISTER** and "Bob Juiceton" discussed the prices of Anabolic Steriods for purchase. **LEISTER** explained to "Bob Juiceton" that he would like a quote on several different types of Anabolic Steroids for purchase. On December 13, 2018, "Bob Juiceton" quoted **LEISTER** $2,945 for the order he requested. "Bob Juiceton" informed **LEISTER** that he would begin to ship the steroids to **LEISTER** over the course of the next few days. On December 28, 2018, **LEISTER** messaged "Bob Juiceton" asking him when the package would be shipped. On December 29, 2018, "Bob Juiceton" told **LEISTER** he was sending him the tracking information, and then sent **LEISTER** a picture of a USPS Priority Mail Express package tracking slip with a tracking number. During this conversation, **LEISTER** told "Bob Juiceton" that he had been involved in Silk Road[1] in the past, and had $60,000.00 US currency seized from him by

[1] Your Affiant believes that "Silk Road" is a reference to a website that was an online black market and the first modern darknet market, best known as a platform for selling illegal drugs. It was ultimately shut down by the FBI and its founder was prosecuted in the federal court in New York.

law enforcement. He spoke explicitly about the "Dark Web" with "Bob Juiceton" during this conversation.

b. Month of January 2019 – **LEISTER** continued his conversation with "Bob Juiceton" and on January 3, 2019, **LEISTER** communicated with "Bob Juiceton" about the USPS tracking not updating. **LEISTER** explained to "Bob Juiceton" that he needed the order for an unknown third party, and he was concerned about why the USPS tracking was not updating. **LEISTER** and "Bob Juiceton" discussed the possibility that the package was seized, and **LEISTER** explained to "Bob Juiceton" that he was caught "selling weed" through mail order. **LEISTER** assured "Bob Juiceton" that he knows what to do if he believed that a package was seized by Postal Authorities. On January 7, 2019, **LEISTER** messaged "Bob Juiceton" and informed him that he had received a package that day. The two continued to discuss on various days throughout the month of January 2019 the sale/purchasing of Anabolic Steroids.

c. Month of March 2019 – **LEISTER** messaged a receipt showing the tracking information through the USPS to "Bob Juiceton" on March 12, 2019. On March 14, 2019, "Bob Juiceton" messaged **LEISTER** a photograph of a tracking number, along with the address of the **PREMISES**. On March 23, 2019, "Bob Juiceton" sent **LEISTER** a photograph of a receipt showing a USPS tracking number for a package destined for Glenville, PA. On March 25, 2019, **LEISTER** sent "Bob Juiceton" a screenshot of a text message with a "Larry Armell." In the message "Larry Armell" asked **LEISTER** to "Mail his stuff." **LEISTER** responded "Yeah, it's in the mail."

d. Month of April 2019 – **LEISTER** and "Bob Juiceton" continued to have discussion about anabolic steroids, however no orders were made.

e. Month of May 2019 – "Bob Juiceton" sent **LEISTER** the photograph of another tracking receipt from the USPS, with a tracking number. **LEISTER** and "Bob Juiceton" continued to discuss ordering Anabolic Steroids and, on May 29, 2019, **LEISTER** asked "Bob Juiceton" to send him another large order of controlled substances.

f. Month of June 2019 – **LEISTER** reached out to "Bob Juiceton" and they discussed a package that was held up at customs, and they believed was opened by authorities.

34. Through Facebook, **LEISTER** was also communicating with a subject using the name "Brian Joseph." In the conversation between **LEISTER** and "Brian Joseph" the following was observed:

a. Month of October 2018 – **LEISTER** spoke to "Brian Joseph" about the "Dark Web" and gave a website to log onto on the "dark web" containing information regarding the cycling of anabolic steroids. On October 22, 2019, "Brian Joseph" sent **LEISTER** a photograph of a large quantity of white colored tablets that resembled Schedule IV Alprazolam, more commonly known as Xanax. On October 22, 2019, **LEISTER** asked "Brian Joseph" if he had a list of products for sale, and "Brian Joseph" sent **LEISTER** a menu of both controlled and non-controlled substances they had for sale over the internet. In this menu a large variety of anabolic steroids can be seen, along with Xanax 2mg tablets.

b. Month of February 2019 – **LEISTER** continued to discuss with "Brian Joseph" the purchasing of anabolic steroids and, in one message sent "Brian Joseph" his home address of the **PREMISES**.

35. The Facebook data requested ended at June 3, 2019.

UNITED STATES POSTAL INSPECTORS INVESTIGATION

36. During the month of August 2019, your Affiant enlisted the help of the United States Postal Inspector's Office ("USPIS") in reference to **LEISTER** receiving illicit narcotics through the US Mail. A Special Agent ("SA") of the USPIS learned that **LEISTER** was receiving a high volume of parcels shipped from addresses suspected by the USPIS as "Dark Web" or "Deep Web" addresses. The USPIS SA identified that numerous parcels delivered to the **PREMISES** originated from addresses that were USPIS target addresses of suspected "Dark Web" websites.

37. The USPIS SA identified that, in May 2019 – June 2019, several parcels addressed to **LEISTER** at his residence were delivered from suspected "Dark Web" originating addresses. Notably, one of the dates a suspicious parcel was delivered to **LEISTER** at his residence, was the same date **LEISTER** had shared a photograph of two large sheets of suspected white colored Xanax tablets with the undercover detective through the Wickr application.

38. The USPIS SA identified an incoming parcel to **LESITER** at his residence that he believed contained illicit narcotics and, in August 2019, held the package pending a warrant. After that warrant was issued by a US Magistrate in the US District Court of Harrisburg, Pennsylvania, the package was opened by the USPIS and found to contain several vials of suspected Anabolic Steroids, which were illegal to possess.

INDICTMENT AND ARREST OF JACOB LEISTER

39. On November 19, 2019, **LEISTER** was indicted by a Federal Grand Jury on four counts of violation of 21 U.S.C. § 841(a)(1) and 21 U.S.C. § 841(b)(1)(C) (Distribution of and Possession with Intent To Distribute a Controlled Substance). An arrest warrant was issued

through the court.

40. On November 19, 2019, your affiant submitted for review an affidavit for a search and seizure warrant through the US District Court in Harrisburg, Pennsylvania.

41. The Honorable US Magistrate Martin C. Carlson of the US District Court in Harrisburg, PA reviewed the affidavit, and signed a warrant to search the residence of **LEISTER**, located at 4692 Blue Hill Road, Glenville, PA.

42. The undercover detective arranged to meet with **LEISTER** at an undisclosed location in Manchester, Maryland to purchase approximately 2,000 tablets of Xanax. This communication was done through the "wickr" application. The agreement was made to meet on November 21, 2019, in the early afternoon hours. On November 21, 2019, investigators conducted physical surveillance of the agreed upon meeting place, and identified **LEISTER** pulling into the location in a blue colored Subaru station wagon. Shortly after his arrival, **LEISTER** was taken into custody, pursuant to the arrest warrant.

43. A search of **LEISTER** and his vehicle incident to his arrest was conducted, and investigators located on his front passenger seat a large quantity of Xanax bars, heat sealed and pressed. The manner in which the Xanax bars were stored (flat pressed in a heat sealed plastic wrap), indicated that they had been shipped via the US mail or a similar parcel shipping method. The bars appeared to be packaged in 1,000 tablet bundles.

44. Also located in the passenger compartment of LEISTER's vehicle was an SD digital data storage card (i.e., **Storage No. 2**), and a Samsung Galaxy S8+ cellular telephone (i.e., **Cellphone No. 1**).

SEARCH WARRANT AT LEISTER'S RESIDENCE

45. After taking **LEISTER** into custody, investigators responded to 4692 Blue Hill

Road, Glenville, PA, **LEISTER**'s residence, to execute a search and seizure warrant. After securing the residence investigators located numerous laptops, and other electronics throughout the residence. These electronics also included small digital storage devices, telephone SIM cards, and smart tablets.

46. Located in the living room area of LEISTER's residence, investigators located a DELL laptop with serial number BC05662 (i.e., **Computer No. 1**). The laptop was in the common area of the living room found on a small table.

47. Located in the closet of an unfurnished bedroom, investigators located an HP laptop with no serial number (i.e., **Computer No. 2**), a DELL Inspiron laptop with serial number 70MDBC1 (i.e., **Computer No. 3**), and a DELL laptop with serial number 1Z3RZG1 (i.e., **Computer No. 4**). Also found in that room were several items of personal property believed to belong to LEISTER.

48. Located in the kitchen of the residence with a Samsung Galaxy tablet with serial number A3LSMT17S (i.e., **Computer No. 5**). The tablet was located on top of several personal documents with LEISTER's name on them, including a check book with checks written by LEISTER.

49. Located in the master bedroom identified as the room where LEISTER sleeps were miscellaneous digital storage and sim cards all packaged together (i.e., **Storage No. 1**). These storage devices were found near LEISTER's passport.

50. Also found inside of the master bedroom was documentation suggesting that LEISTER had at least two Cryptocurrency accounts, holding an unknown amount of Cryptocurrency.

51. It was identified that roommate identified as a Ky Creamer had recently moved into

LEISTER's residence, however no personal property of Ky Creamer was located in any other room except a secondary furnished bedroom on the main floor. It is believed that all electronic devices taken from 4692 Blue Hill Road, Glenville, PA, belong to Jacob LEISTER, as he is the listed owner of that residence, and has lived there for approximately 4 years.

CONCLUSION

52. Based upon the information set forth in this Affidavit, your Affiant submits that probable cause exists to believe that the SUBJECT DEVICES (listed in Attachment A) contain evidence of violations of 21 U.S.C. § 841, 846 (Distribution and Possession with Intent to Distribute Controlled Substances and conspiracy to commit the same), 21 U.S.C. § 843(b) (Use of a Communication Facility), and 18 U.S.C. § 1956 (Money Laundering), specifically, the items listed on Attachment B. Your Affiant requests a warrant to search those devices using the Search Protocol in Attachment C.

Daniel Pamer
Task Force Officer
Drug Enforcement Administration

Subscribed and sworn to before me this 11th day of December, 2019.

Beth P. Gesner
United States Magistrate Judge

ATTACHMENT "A"

The SUBJECT DEVICES are as follows:

ITEM	DESCRIPTION	SEIZURE LOCATION
Cellphone No. 1	Samsung Galaxy S8+ IMEI#357725084952929 (photo at Attachment "D")	Seized from the vehicle of Jacob LEISTER
Cellphone No. 2	Samsung Galaxy III Trac Phone FCC ID# A3LSCHI535 (photo at Attachment "E")	Seized from 4692 Blue Hill Rd. Glenville, PA
Computer No. 1	Dell Laptop Serial # BC05662 N-7 (photo at Attachment "F")	Seized from 4692 Blue Hill Rd. Glenville, PA
Computer No. 2	HP Laptop No Serial Number N-12 (photo at Attachment "G")	Seized from 4692 Blue Hill Rd. Glenville, PA
Computer No. 3	Dell Inspiron Laptop Serial #70MDBC1 N-13 (photo at Attachment "H")	Seized from 4692 Blue Hill Rd. Glenville, PA
Computer No. 4	Dell Laptop Serial # 1Z3RZG1 N-14 (photo at Attachment "I")	Seized from 4692 Blue Hill Rd. Glenville, PA
Computer No. 5	Samsung Galaxy Tablet Serial # A3LSMT17S (photo at Attachment "J")	Seized from 4692 Blue Hill Rd. Glenville, PA
Storage No. 1	Miscellaneous Digital Storage Cards and Sim Cards (photo at Attachment "K")	Seized from 4692 Blue Hill Rd. Glenville, PA
Storage No. 2	Sans Disk SD Card (photo at Attachment "L")	Seized from vehicle of Jacob LEISTER

All of the aforementioned electronic devices are in the possession of the United States Drug Enforcement Administration at its Baltimore District Office located at 200 St. Paul Place, Suite 2222, Baltimore, Maryland 21202. This warrant authorizes the forensic examination of the

SUBJECT DEVICES for the purpose of identifying the electronically stored information described in Attachment B.

ATTACHMENT "B"

This warrant authorizes the search and seizure of all records contained within the SUBJECT DEVICES described in Attachment A that relate to violations of 21 U.S.C. § 841, 846 (Distribution and Possession with Intent to Distribute Controlled Substances and conspiracy to commit the same), 21 U.S.C. § 843(b) (Use of a Communication Facility), and 18 U.S.C. § 1956 (Money Laundering), by Jacob LEISTER and his known and unknown co-conspirators since July 1, 2018, including, but not limited to:

a. images;
b. videos;
c. records of incoming and outgoing voice communications;
d. records of incoming and outgoing text messages;
e. the content of incoming and outgoing text messages;
f. voicemails;
g. e-mails;
h. voice recordings;
i. contact lists, including lists of customers;
j. types, amounts, and prices of drugs trafficked as well as dates, places, and amounts of specific transactions;
k. any information related to sources of drugs (including names, addresses, phone numbers, or any other identifying information);
l. data from third-party applications (including social media applications like Facebook and Instagram and messaging programs like WhatsApp and Snapchat);
m. location data;
n. browser history;
o. any information regarding LEISTER's schedule or travel;
p. bank records, checks, credit card bills, account information, and other financial records;
q. evidence of user attribution showing who used or owned the Subject Device at the time the things described in this warrant were created, edited, or deleted, such as logs, phonebooks, saved usernames and passwords, documents, and browsing history.

As used above, the term "records" includes all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form.

ATTACHMENT "C"

Because of the possibility that the files examined pursuant to this warrant will include information that is beyond the scope of what the United States has demonstrated the existence of probable cause to search for, the search shall be conducted in a manner that will minimize to the greatest extent possible the likelihood that files or other information for which there is not probable cause to search is not viewed.

While this protocol does not prescribe the specific search protocol to be used, it does contain limitations as to what government investigators may view during their search, and the searching investigators shall be obligated to document the search methodology used in the event that there is a subsequent challenge to the search that was conducted, pursuant to the following protocol:

With respect to the search of any digitally/electronically stored information that is seized pursuant to this warrant, and described in Attachment B hereto, the search procedure shall include such reasonably available techniques designed to minimize the chance that the government investigators conducting the search will view information that is beyond the scope for which probable cause exists.

The following list of techniques is a non-exclusive list which illustrates the types of search methodology that may avoid an overbroad search, and the government may use other procedures that, like those listed below, minimize the review of information not within the list of items to be seized as set forth herein:

1. Use of computer search methodology to conduct an examination of all the data contained in such computer hardware, computer software, and/or memory storage devices to determine whether that data falls within the items to be seized as set forth herein by specific date ranges, names of individuals, or organizations;

2. Searching for and attempting to recover any deleted, hidden, or encrypted data to determine whether that data falls within the list of items to be seized as set forth herein;

3. Physical examination of the storage device, including digitally surveying various file directories and the individual files they contain, to determine whether they include data falling within the list of items to be seized as set forth herein; and

4. Opening or reading portions of files that are identified as a result of conducting digital search inquiries in order to determine their relevance.